| Responsible Officer: | ISO |
|---|---|
| Responsible Office: | Compliance |
| Origination Date: | 03/17/2016 |
| Date of Revision: | 03/17/2016 |
| Scope: | • All UCR School of Medicine information, in all its forms, regardless of where it resides, who possesses it or who has authority to create, store, transmit or use it;<br>• All Technology Infrastructure owned and/or administered by UCR School of Medicine;<br>• All UCR School of Medicine divisions, including those of UCR School of Medicine subsidiaries, if any;<br>• All UCR School of Medicine facilities, including those of UCR School of Medicine subsidiaries, if any; and<br>• All UCR School of Medicine workforce members, including employees, interns, contractors, consultants, and vendors doing business with UCR School of Medicine including any individuals affiliated with third parties that access UCR School of Medicine systems. |

## I.     Policy Summary

This policy establishes a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. All computer accounts must be password protected to help maintain the confidentiality and integrity of electronic data, as well as, to help protect the UCR School of Medicine compute resources and infrastructure. Passwords to UCR School of Medicine accounts and devices must be kept confidential and must not be shared.

## II.     Definitions

None at the time of publication.

## III.     Policy Text

One-time-use passwords are initially provided to the users for the first account log-on. Users are required to create a new password known only to them immediately after the initial log-on

### A.  UCR School of Medicine NetID

Passwords must:

- Be a minimum of 8 characters in length
- Not be longer than 32 characters
- Have both upper and lower case characters
- Have at least 1 letter(s)
- Have at least 1 digit(s)
- Not be constructed from a dictionary word

- Not be an exact dictionary word match
- Not be your profile ID or name
- Not be your profile ID or name reversed
- Not be your profile ID or name with letters rearranged
- Not be an old password (any of the previous 12 passwords used)
- Not have more than 1 pair(s) of repeating characters
- Contain characters that can be a pattern typed on a Standard (US) keyboard
- Not contain consecutive characters as in "abcd" or arranged on a keyboard "asdfg"

- UCR School of Medicine NetID passwords will expire every **90 days.**
- Each user must have a unique, named, individual UCR SOM NetID
- Network and system administrators will be issued a separate, unique named account specifically for elevated access, as outlined in policy "*Managing Privileged Access.*"

### B. Self-Service Portal
UCR SOM NetID Account holders should set up their challenge questions to facilitate self-service password resets **(**https://password.medsch.ucr.edu/PM/enroll1.asp)
All Information systems must obscure the password during password entry.
Displaying asterisks when a user types in a password is an example of obscuring feedback of password information.
UCR SOM NetID Lockout conditions:
- Users failing to logon after 5 times will experience an automatic lockout,
- Lockout duration will be no less than 30 minutes,
- To unlock accounts before 30 minutes the user must call the HELPDESK and provide ID and answer challenge questions

## IV.     Responsibilities: N/A

## VIII.    Related Information
- SOM 6.0 Privacy and Security Sanctions Policy
- UCR School of Medicine Policy– Managing Privileged Access
- UCR School of Medicine Policy – Security Awareness and Training
- UCR School of Medicine Policy – Workstation Security
- UCR School of Medicine Policy – Encryption Controls
- Document Retention Policy
- UC Record Retention Schedule

## IX.     Revision History:

| Date Revised | Description of Changes | Author | Reviewer | Date Approved |
|---|---|---|---|---|
| 3/15/2016 | Initial Draft | Shawn Kelly | | |
| 3/17/2016 | Update | Shawn Kelly | | |

**Approval(s):**

**Compliance Committee (04/26/2016)**